CLAIMS

What is Claimed is:

1. A method comprising:

detecting an attack by malicious code on a first computer system;

extracting a malicious code signature from said malicious code;

creating an extracted malicious code packet including said malicious code signature; and

sending said extracted malicious code packet from said first computer system to a second computer system.

2. The method of Claim 1 wherein prior to said sending, said method further comprising determining that said extracted malicious code packet is a new extracted malicious code packet.

3. The method of Claim 1 wherein prior to said sending, said method further comprising determining that a maximum number of extracted malicious code packets have not been sent from said first computer system.

4. The method of Claim 1 wherein said extracted malicious code packet is sent from said first computer system to said second computer system on a secure channel.

5. A method comprising:

detecting an attack by malicious code on a first computer system;

creating an extracted malicious code packet including parameters associated with said malicious code; and

sending said extracted malicious code packet from said first computer system to a second computer system.

6. The method of Claim 5 wherein prior to said sending, said method further comprising determining that said

extracted malicious code packet is a new extracted malicious code packet.

7. The method of Claim 5 wherein prior to said sending, said method further comprising determining that a maximum number of extracted malicious code packets have not been sent from said first computer system.

8. The method of Claim 5 wherein said extracted malicious code packet is sent from said first computer system to said second computer system on a secure channel.

9. The method of Claim 5 further comprising determining whether said malicious code is sendable.

10. The method of Claim 9 wherein upon a determination that said malicious code is sendable, said method further comprising extracting said malicious code from a memory location.

11. The method of Claim 10 wherein said extracting comprises copying or cutting said malicious code from said memory location.

12. The method of Claim 10 further comprising appending said parameters to said malicious code after said extraction.

13. The method of Claim 9 wherein upon a determination that said malicious code is not sendable, said method further comprising extracting a snippet of said malicious code from a memory location.

14. The method of Claim 13 wherein said extracting comprises copying or cutting a portion of said malicious code from said memory location.

15. The method of Claim 13 further comprising appending said parameters to said snippet after said extraction.

16. A method comprising:

receiving an extracted malicious code packet from a first computer system with a second computer system; and

determining whether an attack threshold has been exceeded based upon said extracted malicious code packet.

17. The method of Claim 16 wherein upon a determination that an attack threshold has been exceeded, said method further comprising delivering a signature update comprising a malicious code signature.

18. The method of Claim 17 wherein said signature update is delivered to an intrusion detection system.

19. The method of Claim 17 further comprising determining that a maximum number of signature updates have not been sent prior to said delivering a signature update.

20. The method of Claim 17 further comprising creating said signature update.

21. The method of Claim 16 wherein said extracted malicious code packet includes a malicious code signature, and wherein upon a determination that said attack threshold has been exceeded, said method further comprising delivering said malicious code signature to a global analysis center.

22. The method of Claim 21 further comprising determining that a maximum number of malicious code signatures have not been sent prior to said delivering said malicious code signature.

23. The method of Claim 21 further comprising extracting said malicious code signature from said extracted malicious code packet.

24. The method of Claim 16 further comprising determining whether said extracted malicious code packet includes a malicious code signature, wherein upon a determination that said extracted malicious code packet does not include a malicious code signature, said method further comprising extracting a malicious code signature from said extracted malicious code packet.

25. The method of Claim 16 wherein upon a determination that said attack threshold has been exceeded, said method further comprising delivering said extracted malicious code packet to a global analysis center.

26. The method of Claim 25 further comprising determining that a maximum number of extracted malicious code packets have not been sent prior to said delivering said extracted malicious code packet.

27. A computer system comprising:

an intrusion prevention application for detecting an attack by malicious code on a first computer system;

a host signature extraction application for extracting a malicious code signature from said malicious code;

said host signature extraction application further for creating an extracted malicious code packet including said malicious code signature; and

said host signature extraction application further for sending said extracted malicious code packet from said first computer system to a second computer system.

28. A computer system comprising:

an intrusion prevention application for detecting an attack by malicious code on a first computer system;

a host signature extraction application for creating an extracted malicious code packet including parameters associated with said malicious code; and

said host signature extraction application further for sending said extracted malicious code packet from said first computer system to a second computer system.

29. A computer system comprising:

a local analysis center signature extraction application for receiving an extracted malicious code packet from a first computer system with a second computer system; and

said local analysis center signature extraction application further for determining whether an attack threshold has been exceeded based upon said extracted malicious code packet.